



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/749,142	12/27/2000	Thomas Wille	DE000002	4761

24737 7590 04/11/2005

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER

DINH, MINH

ART UNIT PAPER NUMBER

2132

DATE MAILED: 04/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/749,142

Applicant(s)

WILLE ET AL.

Examiner

Minh Dinh

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 December 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 2-4 and 6-14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 2-4 and 6-14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 27 December 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 12/16/2004. Claims 2, 4, 6-7, 9-14 have been amended; claims 1 and 5 have been canceled. The specification has also been amended.

Response to Arguments

2. Applicant's arguments filed 12/16/2004 have been fully considered but they are not persuasive. In response to applicant's argument that it would not be obvious to use the dummy programs of Jahnich in a parallel processing environment because the dummy programs are executed in serial order as disclosed in the Jahnich reference (p. 9, last par), the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

In response to applicant's argument that it would not be advantageous to use the dummy programs of Jahnich in a parallel processing environment (p. 10, 1st par), Jahnich teaches that execution of the dummy programs causes additional advantageous current fluctuations to be observed in a DPA analysis and thus contributes to the confusion of an attacker (col. 6, lines 32-37). Jahnich's teaching is

general in principle and, therefore, is beneficial to any type of execution environment, whether serial or parallel processing.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 2, 4, 7, 9 and 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin et al. (6,658,569) in view of Jahnich et al. (6,725,374).

Regarding claim 7, which is exemplary of claims 2, 4 and 10-13, Patarin discloses a method of operating a data-processing device, with an integrated circuit comprising a central processing unit and one or more co-processors, in which the integrated circuit performs cryptographic operations, characterized in that in performing a cryptographic operation in the integrated circuit, the cryptographic operation is split up into at least two sub-operations and at least two processors perform the sub-operations in parallel and simultaneously (Abstract; Fig. 2, step A; col. 12, lines 6-12 and 31-40), while subsequently corresponding sub-results are combined to an overall result of the overall cryptographic operation (Fig. 2, step B; col. 12, lines 6-12 and 31-40). Patarin does not teach the use of dummy operations when performing a cryptographic operation. Jahnich discloses using dummy programs, whose execution does not

Art Unit: 2132

influence an encryption result (col. 6, lines 32-48); the dummy programs meet the limitation of dummy operations. It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the method of Patarin to use dummy operations when performing a cryptographic operation, as taught by Jahnich. The execution of the dummy operations causes additional advantageous current fluctuations to be observed in a DPA analysis and thus contributes to the confusion of an attacker. Accordingly, the dummy operation is performed in parallel and simultaneously with other sub-operations.

Regarding claim 9, Patarin further discloses that the sub-operations are parts of an encryption in accordance with DES (figures 3a-b).

5. Claims 3, 6, 8 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patarin in view of Jahnich as applied to claims 2, 4, 7 and 13 above, and further in view of Tan (6,490,353).

Regarding claims 3 and 6, Patarin and Jahnich do not disclose that the selection of a processor to perform a cryptographic operation is randomly controlled. Tan discloses that the selection of a processor to perform a certain cryptographic operation is randomly controlled (col. 3, lines 60-64; col. 6, lines 6-12). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the combined method of Patarin and Jahnich such that the selection of a processor to perform a cryptographic operation is randomly controlled, as taught by Tan, so that security could further be enhanced.

Art Unit: 2132

Regarding claims 8 and 14, Patarin and Jahnich do not disclose that the split-up of the cryptographic operation is randomly controlled. Tan discloses that data to be encrypted is segmented into blocks and that the size of each data block and length of the corresponding encryption key for each block are randomly selected (col. 3, lines 8-42); the selection of the block size and the key length meet the limitation of splitting up a cryptographic operation. It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the combined method of Patarin and Jahnich such that the split-up of the cryptographic operation is randomly controlled, as taught by Tan, to increase the degree of difficulty in attacking the encryption system.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,839,847 to Ohki et al.

U.S. Patent No. 6,839,849 to Ugon et al.

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the

Art Unit: 2132

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

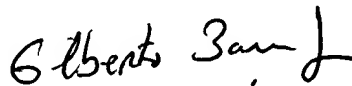
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
4/6/05


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100